

RAPPORT D'ACTIVITÉ

FRAUDE SIGNALÉE SUR FRAUDE- ALERTE.CA

T2

2^e trimestre 2026

Le trimestre en chiffres

573

SIGNALEMENTS

176 975

VUES

164\$

PERTE MÉDIANE

■ OBSERVATIONS

Signalements analysés **393**

Perte médiane **164,70 \$**

Perte moyenne **10 586,61 \$**

Perte maximale **200 000 \$**

Perte minimale **35 \$**

La perte maximale actuellement recensée, soit 200 000 \$, est associée à une fraude à l'emploi impliquant des transferts de cryptomonnaie, et non à une fraude financière.

■ MÉTHODOLOGIE

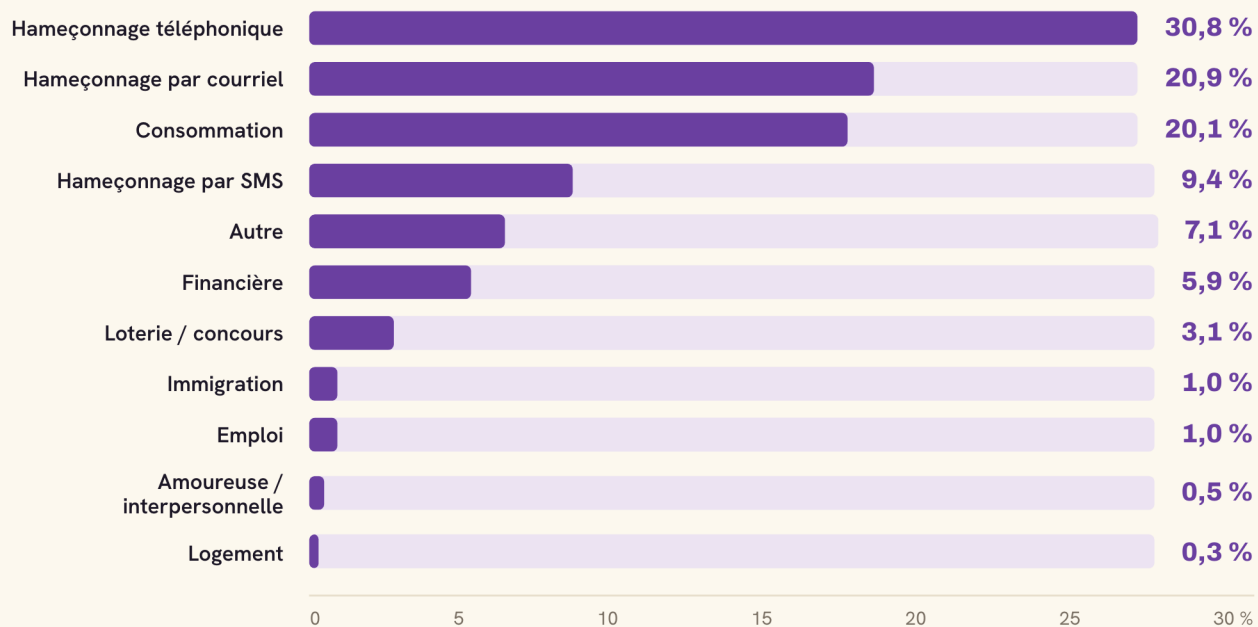
Note — seulement 5,9 % des 393 signalements analysés indiquaient un montant perdu.

Exclusions appliquées à l'analyse :

- Signalements provenant de l'étranger
- Signalements non pertinents ou incohérents

Certains signalements exclus restent disponibles sur Fraude-Alerte, mais n'ont pas été pris en compte dans l'analyse.

Catégories les plus signalées



L'hameçonnage téléphonique constitue la catégorie la plus fréquente, représentant 30,8 % des signalements analysés. Les principaux scénarios concernent l'usurpation de l'identité d'institutions financières, notamment Desjardins et RBC, de services policiers, d'organismes gouvernementaux ou d'entreprises comme Hydro-Québec. Les fraudeurs prétendent généralement qu'une carte bancaire a été clonée ou qu'une transaction inhabituelle a été détectée afin d'obtenir des renseignements personnels, des numéros de carte ou des transferts d'argent. Plusieurs appels silencieux ou de courte durée, parfois perçus comme des tentatives d'enregistrement de la voix, ont également été signalés.

L'hameçonnage par courriel représente 20,9 % des cas : fausses factures, faux avis de paiement ou de transaction, courriels usurpant l'identité de la GRC, de Desjardins, de l'Agence du revenu du Canada ou de fournisseurs de télécommunications. Certains messages utilisent de prétendues menaces judiciaires ou de faux mandats d'arrestation afin de créer un sentiment d'urgence.

Consommation, « autre » et fraude financière

La fraude à la consommation correspond à 20,1 % des signalements et concerne principalement des achats effectués sur des sites de vente en ligne ou des plateformes de petites annonces. Les situations rapportées comprennent des produits jamais livrés, des articles de mauvaise qualité ou non conformes à leur description ainsi que des abonnements cachés.

La catégorie « Autre », qui représente 7,1 % des cas, regroupe notamment des fraudes liées à des services en ligne, des piratages informatiques et des usurpations d'identité. Certains signalements concernent des tests de QI ou d'autres services donnant lieu à des prélèvements ou à des abonnements non autorisés.

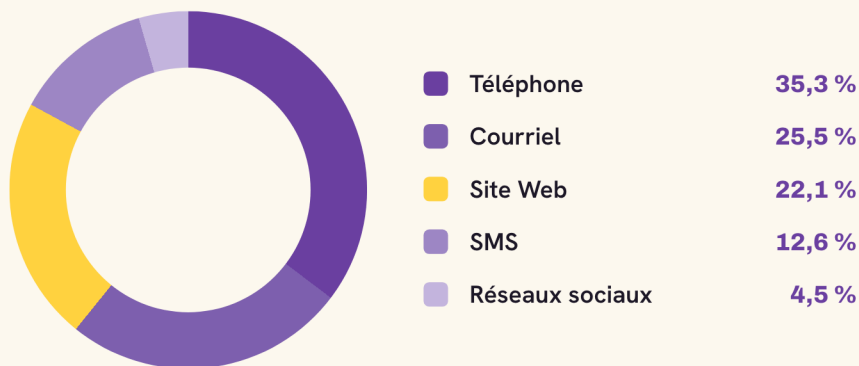
Les fraudes financières demeurent relativement peu nombreuses, représentant 5,9 % des cas. Elles concernent principalement de faux prêts et de fausses occasions d'investissement, notamment dans les cryptomonnaies. Toutefois, la perte maximale actuellement recensée, soit 200 000 \$, est associée à une fraude à l'emploi impliquant des transferts de cryptomonnaie, et non à une fraude financière.

■ TROIS CATÉGORIES, TROIS PROFILS

Consommation	20,1 %
Autre	7,1 %
Financière	5,9 %

À retenir — les fraudes financières et à l'emploi sont peu nombreuses, mais concentrent les montants les plus élevés. À l'inverse, la fraude à la consommation est très fréquente et associée à des pertes unitaires modestes, ce qui explique l'écart marqué entre la perte médiane (164,70 \$) et la perte moyenne (10 586,61 \$).

Par où passent les fraudeurs



Téléphone (35,3 %) — principal canal utilisé par les fraudeurs, parmi les signalements dont le moyen de communication est renseigné. Cette proportion concorde avec la forte présence de cas d'hameçonnage téléphonique : usurpation de l'identité d'institutions financières, d'organismes gouvernementaux et de services publics, ainsi que des appels silencieux ou de courte durée parfois perçus comme des tentatives d'enregistrement de la voix.

Courriel (25,5 %) — deuxième rang. Utilisé pour transmettre de fausses factures, de faux avis de paiement ou de transaction, des demandes frauduleuses de paiement de loyer ainsi que de prétendues convocations policières ou menaces judiciaires. Certains messages usurpent l'identité de la GRC, de Desjardins ou d'autres organisations connues afin de créer un sentiment d'urgence.

Site Web (22,1 %) — principalement associé aux fraudes à la consommation, aux abonnements cachés ainsi qu'aux faux services et investissements. Plusieurs signalements concernent des produits jamais livrés, des articles non conformes à leur description ou des paiements récurrents non autorisés.

SMS (12,6 %) — faux avis de livraison, fausses offres d'emploi, virements Interac frauduleux et prétendues transactions liées aux cryptomonnaies.

Réseaux sociaux (4,5 %) — surtout associés à des annonces Marketplace frauduleuses, à de fausses boutiques et à des publicités proposant des produits à prix fortement réduit.

L'usurpation d'identité

20,9%

des signalements faisaient état de l'usurpation de l'identité d'une organisation connue. Les fraudeurs adaptent leurs scénarios à des organisations crédibles afin de renforcer la légitimité et le sentiment d'urgence de leurs demandes.



Les institutions financières et les services de paiement constituent le groupe d'organisations le plus souvent usurpé, représentant 8,4 % des signalements analysés. Les fraudeurs se font notamment passer pour Desjardins, RBC ou la Banque Nationale afin de signaler de prétendues transactions inhabituelles et d'obtenir des renseignements personnels ou des transferts d'argent. Les services policiers, notamment la GRC et le SPVM, ont été usurpés dans 1,3 % des cas : fausses accusations, prétendus mandats d'arrestation ou fausses enquêtes financières visant à effrayer les victimes.

■ REQUÊTES

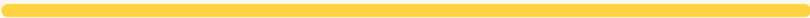
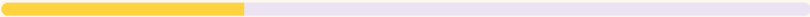
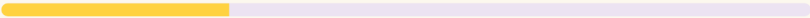
Ce que les internautes ont cherché

La majorité des requêtes portent sur des numéros de téléphone, ainsi que sur des boutiques en ligne.

■ NUMÉROS DE TÉLÉPHONE LES PLUS VÉRIFIÉS

514 375-2413	9 113 REQUÊTES	438 238-1439	3 957 REQUÊTES
873 730-1016	2 174 REQUÊTES	514 416-6465	1 408 REQUÊTES
581 781-7510	1 140 REQUÊTES	844 518-7852	1 048 REQUÊTES

■ BOUTIQUES EN LIGNE LES PLUS RECHERCHÉES

Nevara		3 863
Novaya Québec		1 172
Nordaska		1 085

D'autres signalements concernent également des boutiques telles que Vivaura, Boutique Éléance et Gencivie. Plusieurs misent sur une image locale ou crédible afin de renforcer leur apparence de légitimité et d'inciter les internautes à leur faire confiance.

■ LA PLATEFORME ELLE-MÊME

Requêtes visant « Fraude-Alerte »	1 015
Vues totales du trimestre	176 975

Lecture — le réflexe de vérification passe d'abord par un numéro de téléphone ou le nom d'une boutique. Fraude-Alerte a elle-même fait l'objet de 1 015 requêtes, signe d'une recherche directe de la plateforme.

Comprendre les catégories

Hameçonnage téléphonique

Appel frauduleux visant à tromper les destinataires pour leur voler des informations personnelles, financières ou des identifiants de connexion.

Hameçonnage par courriel

Courriel frauduleux visant à tromper les destinataires pour leur voler des informations personnelles, financières ou des identifiants de connexion.

Hameçonnage par SMS

Messages texte frauduleux visant à tromper les destinataires pour leur voler des informations personnelles, financières ou des identifiants de connexion.

Fraude à la consommation

Fraudes impliquant des sites de vente en ligne frauduleux usurpant l'identité d'entreprises légitimes, basés sur le dropshipping, ou des sites de petites annonces (Marketplace, Kijiji, etc.).

Fraude financière

Fraudes liées à l'investissement, à l'investissement en cryptomonnaies, ou aux offres de prêts d'argent.

Fraude à l'immigration

Fraudes exploitant des démarches d'immigration : faux services de représentation, frais illégitimes ou prétendues procédures accélérées.

Fraude à l'emploi

Fausse offres d'emploi impliquant l'achat de cartes-cadeaux, l'encaissement de chèques frauduleux, des transferts de cryptomonnaie ou l'arnaque à la tâche.

Fraude au logement

Fausse offres de logement à loyers attractifs, ou courriel frauduleux demandant le paiement d'un loyer.

Fraude amoureuse / interpersonnelle

Un individu gagne la confiance et l'affection de sa victime en prétendant une relation romantique, dans le but d'obtenir de l'argent ou des informations personnelles.

Autres

Fraudes impliquant des services en ligne, des piratages informatiques ou des usurpations d'identité, y compris les tests de QI et services donnant lieu à des prélèvements non autorisés.